The Connected Apple Family

Discover the Rich Apple Ecosystem of the **Mac**, **iPhone**, **iPad**, and **AppleTV**

JEFF CARLSON and DAN MOREN

The Connected Apple Family

Discover the Rich Apple Ecosystem of the
Mac, **iPhone**, **iPad**, and **AppleTV**

JEFF CARLSON and DAN MOREN

PEACHPIT PRESS

The Connected Apple Family:
Discover the Rich Apple Ecosystem of the Mac, iPhone, iPad, and Apple TV

Jeff Carlson and Dan Moren

Peachpit Press
www.peachpit.com

To report errors, please send a note to errata@peachpit.com
Peachpit Press is a division of Pearson Education

Editors: Clifford Colby and Scout Festa
Production editor: David Van Ness
Copyeditor: Scout Festa
Compositors: Jeff Carlson and Danielle Foster
Indexer: Valerie Haynes Perry
Cover Design: Aren Straiger
Interior Design: Mimi Heft

ISBN 13: 978-0-134-03624-3
ISBN 10: 0-134-03624-7

9 8 7 6 5 4 3 2 1
Printed and bound in the United States of America

To Kimberly and Ellie, who can never receive too many dedications.
—Jeff

To my parents, Harold and Sally, for their unfailing encouragement and a lifelong love of books.
—Dan

Acknowledgments

Our sincere thanks go out to the following people, who made it possible for us to produce this book:

Cliff Colby, for pushing the project into existence at Peachpit Press and moving the publishing machinery as needed to allow us to do the book

Scout Festa for her keen copyediting and proofing skills

Valerie Haynes Perry for writing the index (an underappreciated art)

David Van Ness for coordinating the book's production

Danielle Foster for her layout assistance

Mimi Heft for designing an excellent book and template design

Heidi Blondin, Bert Hopkins, Logan Blondin, and Eliana Carlson for being fantastic models

Everyone involved in printing, binding, and shipping the print book around the world

Contents

Introduction

In the early days of personal computing, using a computer was simple.

Typically you had only one computer. All you had to do was learn how to operate that computer and the software you put on it, and you'd be set.

Well, come to think of it, that was often pretty darn complicated. You had to know which commands to type, which components to install, and more often than not, have a little programming experience under your belt.

And then things started getting easier, at least from the point of view of the people buying and using computers. The Macintosh was introduced as the "computer for the rest of us," with its graphical user interface that describes what we still see today (on Windows PCs, too): mouse pointers, icons, folders and files, clicking-and-dragging.

The Mac made computers friendly without sacrificing processing power, and then the iPhone and iPad made things easier still: People don't have to worry about underlying file systems or obscure network protocols. Children immediately understand how to use the touch interface of iOS.

Today, with an array of devices—computers, phones, tablets, fitness sensors, and wearables such as the upcoming Apple Watch—"computing" has merged into our everyday activities. When you look up driving directions on your iPhone, you're tapping into a powerful computer connected to a worldwide wireless network. We don't think of it as "working with a computer," because it is, from our point of view, a simple task.

And yet, computing is still difficult.

The products are all designed to work together—look at Handoff or AirDrop for passing documents among devices, or iCloud for syncing data—but how? Apple introduced Family Sharing in iOS 8 and OS X Yosemite to finally help families and friends centrally manage apps and media, but the feature carries a few significant limitations (for example, a user can join a family group only twice per year).

This book is your guide through the Apple ecosystem (or "geekosystem," as one friend described it), revealing the best ways to connect these devices.

Notes About This Book

We're making a few assumptions about you, dear reader, to make sure we're all on the same page:

- You have more than one Apple device, and probably more than one person using those devices.
- You know the basics of using Apple's products. We don't expect you to be an expert, but as long as you can get around easily, you're good.
- Most likely, you're the one who has volunteered (or has been tasked) as the go-to person expected to understand all this and set it up for everyone else. In Apple's parlance, that makes you the *Family Organizer* (we'll go into more detail in Chapter 1). If you're not, this book is still helpful in making Apple's ecosystem work—for example, if you're not using the Family Sharing feature, or you know that one day you may find yourself the Family Organizer.
- You and the members of your Apple family—which can be a mix of blood relatives and friends—are running OS X Yosemite (version 10.10) on Macs and iOS 8 on any iPhone, iPad, or iPod touch devices.

As you read, you'll run into examples where we've adopted general terms or phrases to avoid getting distracted by details. For example, we may refer to the "computer" or the "desktop" as shorthand for any traditional computer that isn't an iPad or iPhone.

The same general rule applies to iPad and iPhone models. For example, the iPad mini, despite its size, is still a fully functional iPad, so when we refer to "iPad" in general it applies to the iPad mini as well as to the larger, flagship model. Similarly, we don't always refer to specific models.

We also frequently refer to just the iPhone even though the information applies equally well to the iPod touch. We're not being lazy, for two reasons: If we had to always type "iPhone, iPad, and iPod touch," we'd go quickly insane. Also, as we write this, the latest iPod touch Apple sells is the fifth-generation model, which was originally released in 2012. We suspect that unless Apple has something up its sleeve, the iPod touch as we know it will soon disappear.

When directing you to specific areas within iOS and OS X, we use a short-hand for locating them. For example, to access the preferences for the

Camera app, we'll point you to **Settings > Photos & Camera**. That translates to "open the Settings app and tap the Photos & Camera button" (1).

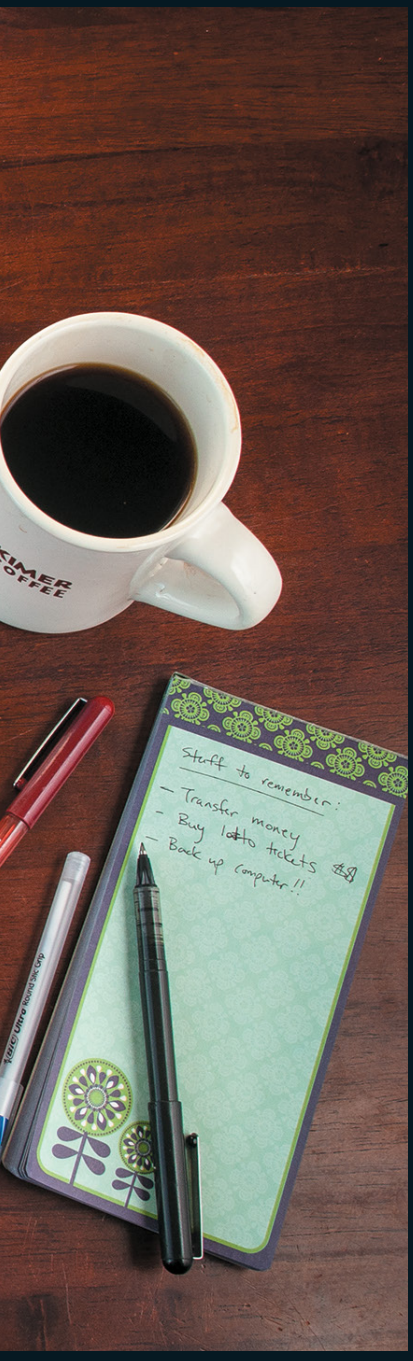
On the Mac, settings are called preference panes and found in System Preferences. So when we ask you to open the iCloud preference pane, it means "open System Preferences and click the iCloud icon" (2).

1 Photos & Camera settings on the iPad

2 Accessing the iCloud preference pane on OS X

This page intentionally left blank


1Password File Edit View Item Window Help
Mon 1:07 PM
danshotfirst.com
DAN SHOT FIRST
Clockwise 62: Light at the End of the Pipe
Posted on November 13, 2014
I'm new to 1Password
I've used 1Password before
AMAZON.COM
123456
Psswrd2
MAC
abc123
Bank:
"password"
(no quotes)
iTunes
000000
iloveyou



CHAPTER 4

Passwords and Security

"Security" used to refer solely to one's physical safety, such as having good door locks and perhaps a home security system. But in our modern world of hacks and malware and phishing, security increasingly focuses on the important information stored on your computer and devices. You can take concrete steps to keep burglars out of your house, but if a malicious entity steals your credit card information—usually from a hacked retailer, not directly from you—your bank accounts could be drained without you even knowing about it.

Understand at the outset that we're not going to sugarcoat security in this chapter. The days when you could choose a pet name as a password, or use the same password for more than one Web site or service, are long over. Security is now a fact of daily digital life.

The good news is, you're not powerless against these threats. In fact, employing good passcodes, using the security features of iOS and OS X, and making a few smart decisions ahead of time goes a long way toward keeping you and your family members safe from technological threats.

Passcodes on iOS

Set a passcode on your iOS device.

No ifs, ands, or buts.

Yes, some friends or family members may protest at having to enter a code every time they want to use their iPhone or iPad, but it's worth pointing out that they probably wouldn't leave valuables in plain view and the door unlocked when they leave the house.

By default, iOS prompts you to create a passcode when you first activate your device, as well prompting you to enable Touch ID if your device supports it. The latter will certainly be easier for most folks, but remember that it's no excuse for not creating a secure passcode—in fact, the convenience of Touch ID gives you a great opportunity to create an even more secure passcode, since you won't have to enter it as often.

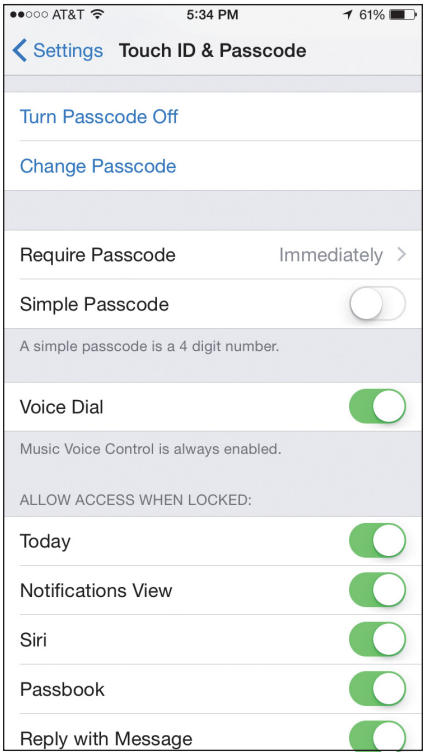
Since iOS requires only a four-digit passcode, entered on a standard number pad, the ability to create a truly secure code might seem limited. However, you can increase the security by choosing a passcode that is much more difficult for someone to crack:

1. Go to Settings > Passcode. (On devices that include a Touch ID sensor, the setting is called Touch ID & Passcode.)
2. Enter your current passcode (because you have one, right?).
3. Slide the toggle next to Simple Passcode to Off (4.1).

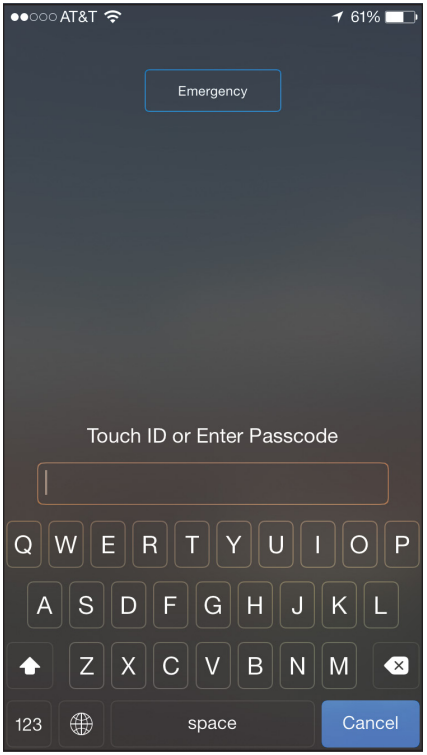
This lets you use passwords composed of numbers and other characters, and have them be of any length. When iOS prompts you for your passcode, instead of giving you the number pad you're shown a full keyboard (4.2).

► **TIP** If you prefer the speed of entering numbers, you can deactivate Simple Passcode, as instructed, and set your passcode to a longer string of just numbers. When iOS asks you to enter your passcode, you still get the number pad. On the downside, this could alert a potential hacker to the fact that your passcode doesn't contain non-number characters, so you should make it even harder to guess.

► **NOTE** A passcode isn't just a door to keep unauthorized people out. When you set up a passcode, all data on the device is encrypted. If, for example, someone were to get hold of your iPhone, open it up, and attempt to access the memory chips directly, the information would be scrambled.



4.1 Passcode settings



4.2 Unlocking with a passcode

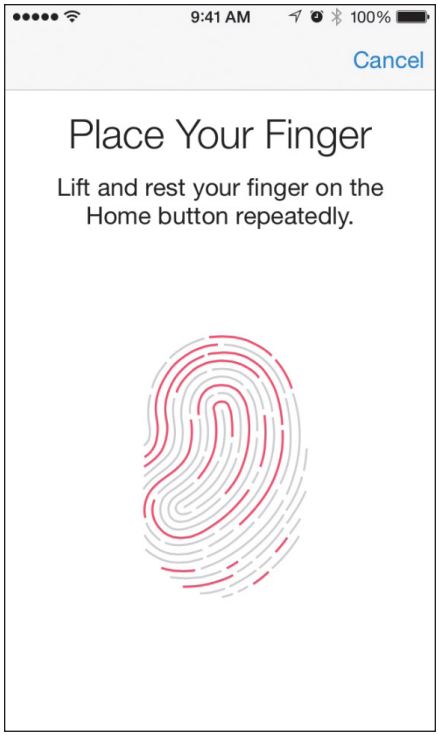
Do You Have Touch ID? Use It

Touch ID is more than just a convenient trick for unlocking your iPhone or iPad. If you own an iPhone 5s, iPhone 6, iPhone 6 Plus, iPad Air 2, or iPad mini 3, you were asked during initial setup to scan your fingerprint for Touch ID. That fingerprint image is stored in a section of the device's processor called the Secure Enclave, which, in addition to having a cool name, is inaccessible by other areas of the system except in very specific circumstances. The print is never shared outside the device (such as via iCloud).

With Touch ID, you can verify purchases from the App Store and iTunes Store without entering a password. App developers can also take advantage of the feature—for example, 1Password can be opened by pressing the Touch ID sensor (the Home button). (We cover 1Password later in this chapter.)

You can configure up to five fingerprints for Touch ID. That's handy for using, say, your left thumb as well as your right thumb, but you can also set up a fingerprint for someone you trust, like a spouse or parent.

1. Go to Settings > Touch ID & Passcode.
2. Enter your passcode.
3. Tap Add a Fingerprint.
4. Follow the instructions for placing your finger on the sensor to read it (4.3).



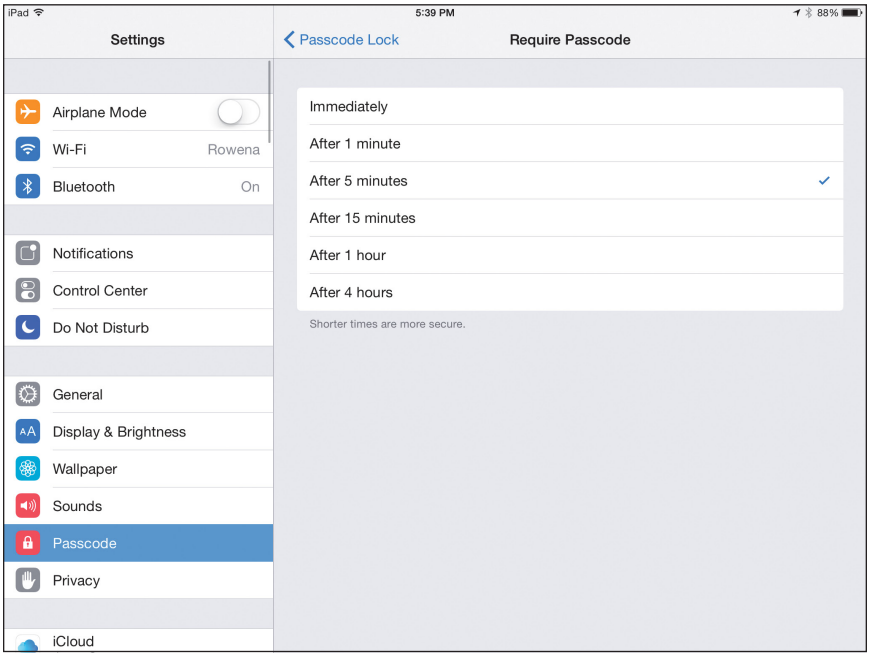
4.3 Setting up Touch ID

5. When the print is stored, optionally tap it in the Fingerprints list and give it a name that's more descriptive than "Finger 2."

► **NOTE** We've heard of a few occasions where Touch ID becomes less responsive over time, although recent iOS updates seem to have improved the situation. If you run into this problem, go to Settings > Touch ID & Passcode, delete the existing fingerprints, and set them up again.

Additional Passcode Options

iOS also allows you to choose how often your passcode is required, assuming you're not using Touch ID. This dictates how long your iOS device needs to be locked before once again prompting you for your passcode. Options range from Immediately to After 4 Hours **(4.4)**.

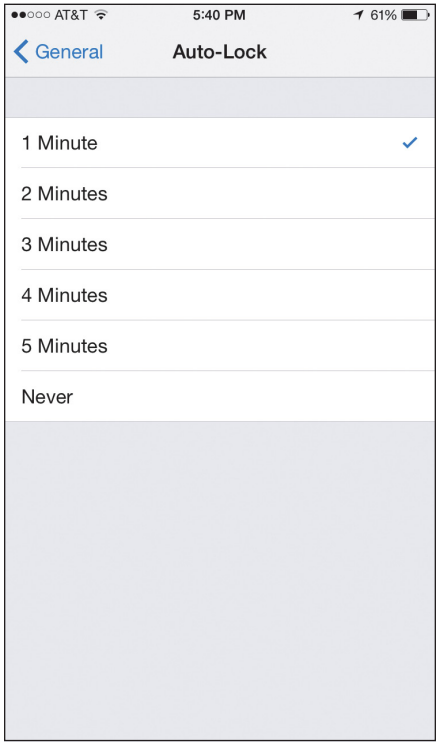


4.4 Choosing when the passcode goes into effect

In general, the smaller the interval, the more secure your device will be. Granted, it can be annoying to have to enter a lengthy passcode every time you want to use your iOS device, but that convenience is balanced against the security of your device should it fall into the wrong hands. For a device that may not leave your house very often—an iPad used by kids, perhaps—you may be able to get by with the After 1 Minute or After 5 Minutes options, but again, if you carry your iPhone with you everywhere, Immediately is the best option. If you've enabled Touch ID, it's also the only option.

The other setting to consider, which *isn't* part of the Passcode section of Settings, is device Auto-Lock, which can be found under Settings > General. This is where you can set how long it takes your iOS device to

automatically lock itself—turn off the screen, and so on (4.5). Again, shorter times generally help maintain better security.



4.5 Choosing when the device locks itself

The Settings > Passcode section also allows you to control whether or not certain features are active on your iOS device when it's locked. On the iPad, this includes features like the Today and Notifications views of Notification Center and Siri; on the iPhone, it also includes the Reply with Message function when you receive a call, and Passbook.

Finally, if your iOS device contains particularly sensitive data, or you are very concerned about nobody getting access to your information, you can enable the Erase Data option, which will delete all content on your device after 10 incorrect passcodes are entered.

▶ **TIP** The Erase Data option is particularly unforgiving. Keep in mind that if your household contains, say, a young child who might have access to your iOS device and may try to guess your passcode or even enter random information, you could end up with a wiped device pretty quickly.

The Elements of a Good Passcode

Password hygiene is important, and iOS device passcodes are no exception. In fact, given that most of us carry our iPhones with us wherever we go, and that they often contain access to our email, contacts, text messages, and banking and other accounts, it's even more critical that they be well protected.

A good password is, ideally:

- **Easy to remember.** Having a password so complicated that it must be written down defeats the very point of a password. Using letters, numbers, and special characters all contribute to making your password harder to guess.

▶ **TIP** One way to make an easy to remember password is to take a phrase, song lyric, or quote, and use the first letter of each word and then add on a piece of punctuation and a number. For example, "Help me, Obi-wan Kenobi, you're my only hope!" could become "hmokymoh!4".

- **Hard to guess.** As tempting as it might be to use your pet's name, your birthday, or your mother's maiden name, all of these facts are surprisingly easy to find with just a modicum of Internet research.
- **Not reused.** The passcode you use to open your iPhone shouldn't be the same as what you use on any other site or service.

But wait, you may be saying, didn't we argue at the beginning of this chapter to *not* choose passwords that are easy to remember? You're correct! In this case, we're talking only about choosing the passcode that unlocks your device. When it comes to passwords for Web sites and services—especially critical accounts such as your bank or other financial sites—you want the security that a truly randomly generated password provides. We go into that later in this chapter.

Mac Security

Passwords are, of course, no less important on OS X. Again, how seriously you take security may depend on a number of factors, such as whether your Mac is a desktop or laptop, where it's located, who has access to it, and what information is stored on it. A computer left in your living room, to which all of your family members have access, for example, likely has different expectations of privacy and security than a personal laptop used for work.

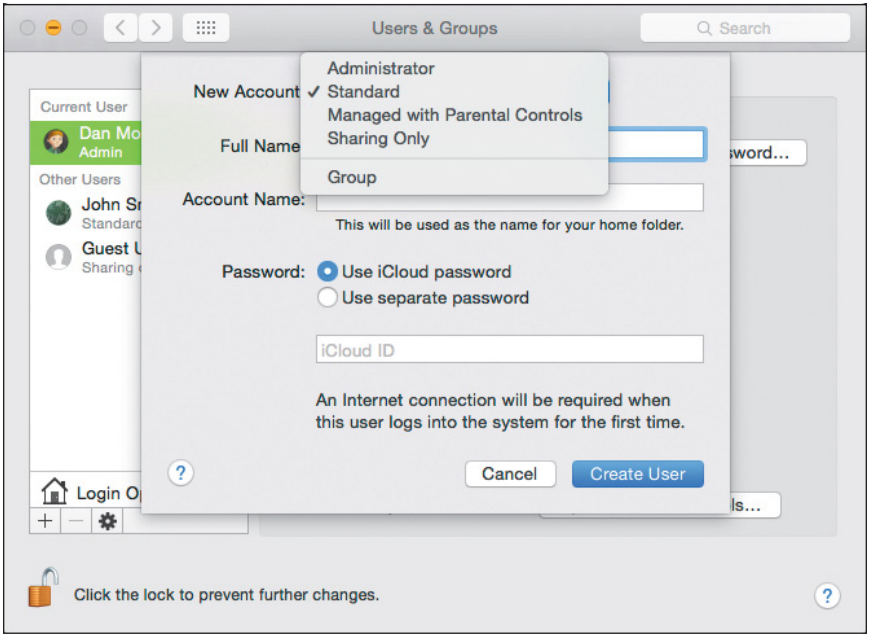
User security

Mac security is managed in a couple different places in OS X. The Users & Groups preference pane in System Preferences lets you create users with different levels of privilege. In general, if your computer is in use by more than one person, it's a good idea to create multiple accounts, both for the convenient use of certain features and for security.

▶ **TIP** Even if you're the only person using your computer, it's useful to create a new user account that remains basic for testing. If something is crashing under your regular user account, for example, you can restart the computer using the test account and see if the problem persists. It's a good way to see if any background processes (applications that run behind the scenes) are causing the issue.

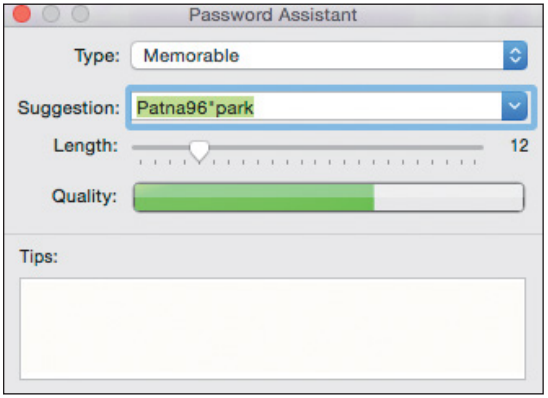
To create a new account, do the following:

1. Open System Preferences and click the Users & Groups button.
2. Click the Add (+) button at the bottom of the user list. You may need to first click the lock icon below the list and provide your current administrator password to enable the Add button.
3. From the New Account pop-up menu, choose one of four types of user accounts: Administrator, Standard, Managed Account with Parental Controls, and Sharing Only **(4.6)**. The Standard account suffices for most common uses, although certain tasks—some software installation, for example—require that an administrator's password be provided. A managed account allows another user, such as a parent, to restrict exactly which features, functions, and capabilities are available. (You can also convert a Standard account to an Administrator or Managed Account after the fact, or vice versa.)
4. Enter the user's full name; an account name is provided automatically based on what you typed, but you can change that if you want.
5. Under OS X Yosemite, you can choose whether or not an account's password should be the same as the person's iCloud password. In fact, if you set up a new user under Yosemite, the default action is to use your Apple ID. However, we recommend creating a separate password instead; if your iCloud account is compromised, your Mac would also be vulnerable or rendered inaccessible to you. Click the Use Separate Password button.



4.6 Setting up a new Standard user account

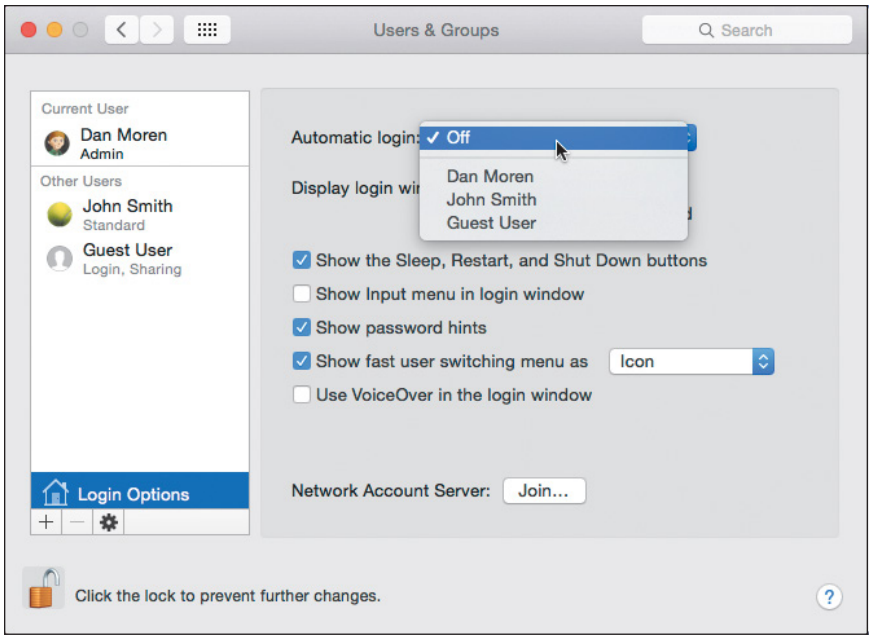
6. Enter a password in the first field (marked with the gray "Required" label); OS X's Password Assistant, the key button to the right, will gladly help you generate one if you need help (4.7). You can change the password later in the Users & Groups pane or in the Security & Privacy pane.



4.7 Password Assistant creates strong passwords.

7. Click the Create User button.

Once you've created a user with a password, you can opt to have your Mac automatically log in to a certain user account when it's booted up, without requiring a password. In the same Users & Groups pane, select Login Options, and then pick an account from the Automatic login drop-down (4.8). This option is useful for a Mac that's primarily used by one person in one location; it's not a good choice for a MacBook you take out of the home or office, since it gives anyone access to your data.



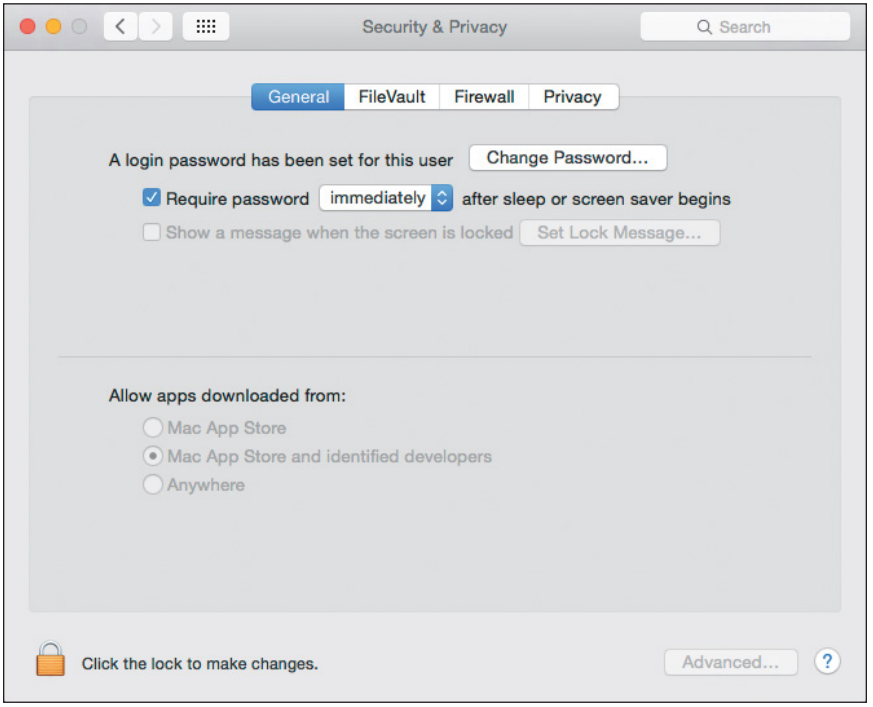
4.8 Turn off Automatic Login on mobile Macs.

▶ **NOTE** If you've enabled FileVault encryption—more on it later—automatic login isn't available as an option for security reasons.

The Login Options section of Users & Groups can additionally be used to configure what's in the login window: whether a full list of users is displayed or simply fields for a username and password. You can also choose to view or hide the Sleep, Restart, and Shut Down buttons, the Input menu, and password hints.

Security & Privacy preferences

Additional options related to passwords and security can be found in the Security & Privacy preference pane of System Preferences. Since it deals with security, the pane includes the same ability to change the password of the currently logged in user as in the Users & Groups pane. You can also choose—as on iOS—how soon a password is required after your Mac goes to sleep or the screen saver starts. Options range from Immediately to 8 hours (**4.9**). Again, shorter intervals, while sometimes less convenient, ensure tighter security. (You can control how long your computer is inactive before triggering the screen saver or display sleep in the Desktop & Screen Saver or Energy Save preference panes, respectively.)



4.9 Choosing how quickly to engage the password request

The Security & Privacy preference pane also allows you to display a message on the login screen, such as contact information in the event that your computer is misplaced or stolen.

One of the most abused attack vectors for malware is convincing people to launch applications that are actually Trojan horses—normal-looking apps that harbor a destructive payload to which the unsuspecting user grants access to the system. Apple's response to this threat is to restrict what can be installed by default. If an installer or an application downloaded from the Internet doesn't match the criteria you specify, OS X does not allow it to be run.

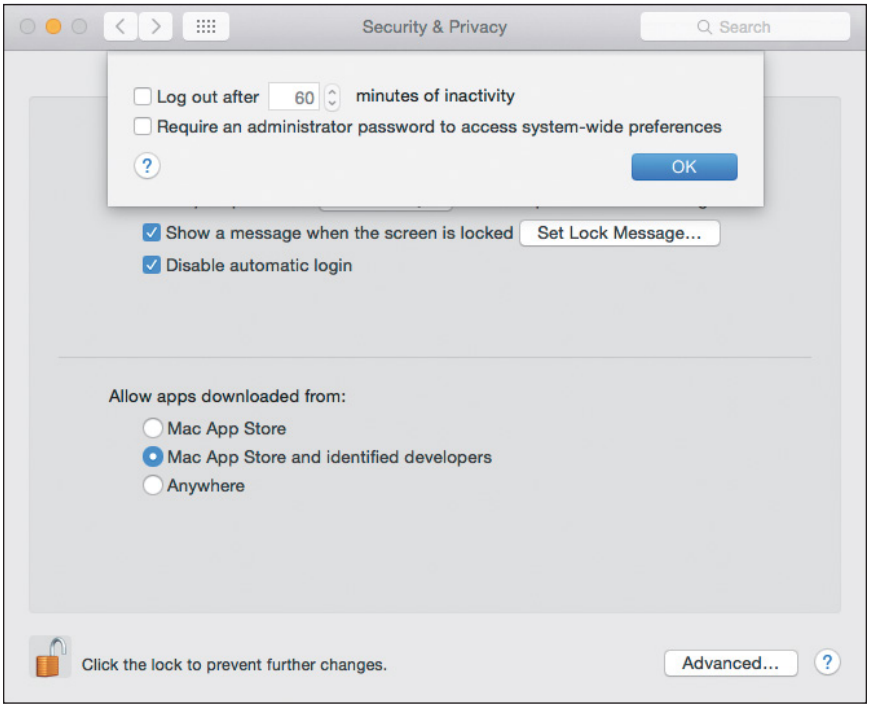
The Allow Apps Downloaded From setting offers three options:

- **Mac App Store.** Apple must approve any software sold through the Mac App Store, so these applications are safe.
- **Mac App Store and Authorized Developers.** Not every company sells its products through the Mac App Store, but Apple maintains a list (which is automatically kept up to date on your Mac) of developers that have passed a certification process.
- **Anywhere.** Choosing Anywhere effectively turns off this line of defense against potentially dangerous applications. It's up to you to make sure the software you install is safe. That doesn't mean anything not authorized or sold from the Mac App Store should be disregarded; it just puts the responsibility in your hands.

Note that this setting applies only to the first time a program is launched or installed. It won't prevent a bad app from running entirely. OS X assumes that if you allowed it to run once, the app must be okay. (A more cynical view is that if you did install malicious software, the damage is already done.)

▶ **TIP** We keep this option set to Mac App Store and Authorized Developers to provide a screen of safety, but there's a workaround for installing unauthorized apps you know are safe without making a trip to the Security & Privacy preference pane: In the Finder, Control-click the app or installer and choose Open. In the warning dialog that appears, you can choose to go ahead with the action.

Clicking the Advanced button in Security & Privacy also gives you access to three other security options **(4.10)**: an auto-log out action, with the ability to choose how many minutes of inactivity before it triggers; whether or not any system-wide preferences (those not specifically linked to the current user account) require an administrator password; and, if the Mac is equipped with an infrared receiver, the ability to disable commands from IR remotes.



4.10 Advanced security settings

FileVault

Having a strong password on your Mac is a good first step, but what's to prevent somebody malicious from simply pulling the hard drive out of your computer and accessing the data on it? In that scenario, there'd be no need to log in, rendering all your passwords moot.

That's where OS X's FileVault comes in. FileVault encodes your Mac's entire disk with powerful encryption, making it incredibly difficult—if not outright impossible—to access without your account credentials or a secret key you set. While it may not be out-and-out bulletproof, it ought to keep anybody short of a particularly determined interloper out of your files.

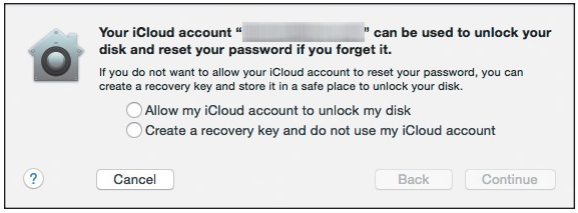
The best thing about FileVault is that it does all its work out of sight. Once you set it up, you'll never really notice its presence.

► **NOTE** Not to bore you, but technically the feature we're talking about is FileVault 2. Apple introduced the original FileVault in an older version of OS X that encrypted just the user's Home folder, which turned out to be a cumbersome implementation. Now, FileVault under OS X Yosemite (and as far back as OS X Lion) performs whole-disk encryption.

Configuring FileVault takes just a few steps.

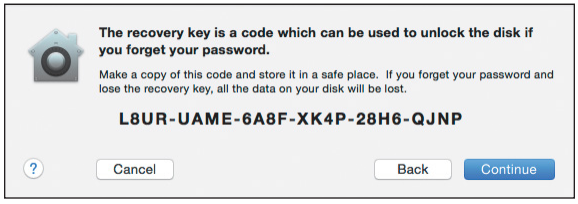
1. Go to the Security & Privacy preference pane in System Preferences and select the FileVault tab.
2. If FileVault is not yet enabled, you'll see a button prompting you to Turn On FileVault. (If the option is grayed out, click the padlock icon and enter an administrator username and password before proceeding.)

► **NOTE** When you enable FileVault, you'll first be presented with two options: to allow your iCloud account access to unlock your disk and reset your password, or to create a recovery key (4.11). While the former is certainly a convenient option, some users may not wish to tie their computer's security to their online account. The recovery key is not stored online, which means you have to find a safe, secure place to keep it, in case you require it later. Both options have their own advantages and disadvantages: which you choose depends on your own personal situation.



4.11 Choose how to unlock FileVault if the password is lost.

3. If you opt to create a recovery key, the next pane displays it (4.12). Make a copy of the key, either written down somewhere secure (a safe or even a safe deposit box), and/or store it in a safe digital location, such as a password manager.



4.12 FileVault recovery key

4. Enter the password for any user accounts on the device beyond the one that is currently enabled. (That, among other things, prevents pranksters from, say, encrypting someone's disk because they left their account logged in.)
5. Once you've logged in all the current users, click Continue. Your Mac prompts you to Restart in order to begin the encryption process.

Upon restarting, you're prompted for your account password. Once you log in, the encryption process begins in the background. Again, it happens transparently; you don't need to do anything, and your other activities shouldn't be affected while the encryption is in process. You can check the progress of the encryption by going to the FileVault section of the Security & Privacy preference pane; a progress bar reflects how much of the disk has been encrypted, and how much is left to go.

Once FileVault is finished with its encryption, the only difference you will notice is that OS X prompts you to log in as soon as you start your computer, rather than once the OS has loaded. You'll see a slightly different login screen—all gray, rather than a translucent one that shows your desktop image behind it.

▶ **NOTE** FileVault explicitly protects your Mac when it's shut down. Once you've logged in, the disk is decrypted in order for you to actually use the machine. So if you use FileVault, keep in mind that you'll still want to protect it with a powerful password and make sure to control physical access to it.

Master Password

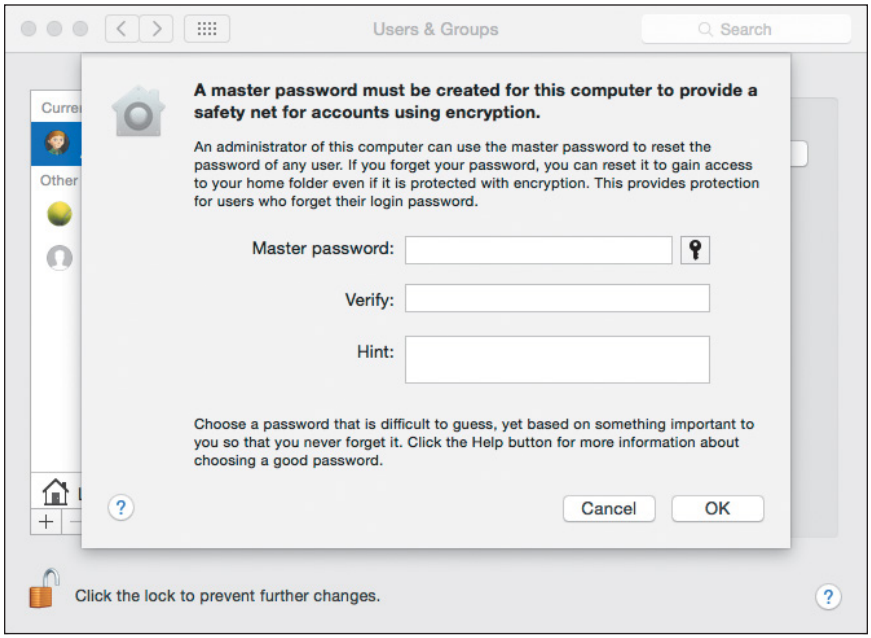
People forget their passwords. It happens. OS X provides a variety of ways to reset passwords: Administrators can reset passwords for other admins, as well as for standard, managed, and sharing accounts; if you've enabled it, you can also reset your password using your Apple ID, which is Apple's recommended method for recovering a forgotten password.

One additional option is to create a master password for your machine, which you can use as a sort of override to reset any user account password—even on an account protected by FileVault.

To set a master password, do the following:

1. Go to the Users & Groups preference pane and click the gear icon at the bottom of the list.

2. Choose Set Master Password, and you'll get a familiar-looking dialog.
3. Enter and verify the master password, along with an optional password hint (4.13). Click OK.



4.13 Setting up a master password

Once a master password is set, if you attempt to log in to an account and fail several times, you'll be prompted to use the master password and create a new password for that account. You can change your master password by going back to the Users & Groups pane and choosing Change Master password from the gear icon, but keep in mind that you'll need to provide the current master password in order to do so.

iCloud Keychain

If you're following good password hygiene—making complex passwords that you don't reuse—you're going to rather quickly run up against the limitations of human memory. Fortunately, OS X provides a solution for not only remembering your passwords but for keeping them all in sync across your various devices: iCloud Keychain.

The Keychain itself dates back to the classic Mac OS, but it's a staple of OS X. It's a secure database for storing all of your passwords for various accounts, Web sites, and so on, all of which can be accessed by typing a single master keychain password—usually the same as your OS X account password.

Starting in iOS 7 and OS X Mavericks, Apple rolled out iCloud Keychain, which lets you sync those passwords—as well as Wi-Fi networks, some credit card information, and other information such as mail, contacts, and calendar accounts—across your Macs and iOS devices, ensuring that the right data is always there when you need it.

Use a VPN When Mobile

If you or other members of a Family Sharing group are at all mobile, you should use a VPN (virtual private network) when connecting to public Wi-Fi hotspots. When you take advantage of a wireless network in a location such as a coffee shop, hotel, or airport, you often hop onto unprotected networks. It's fairly easy for a malicious person to scan all of the wireless traffic for personal information and passwords—that's true even for Wi-Fi networks that require a password.

Think of a VPN as an encrypted tunnel between your computer or iOS device and destinations on the Internet. All of your data is encrypted, so even if someone is snooping the network, they can't do anything with the data you generate. Many companies require employees who work remotely to sign in via a VPN to ensure that potentially valuable work information stays secure.

A VPN used to be a tool that required a computer science degree to set up, but fortunately the real computer scientists are making the tools easier to use. Jeff, who works often at coffee shops, swears by a product called Cloak (getcloak.com), which works on the Mac and on iOS. It's easy to set up, but more importantly, it automatically detects when you connect to an untrusted network and temporarily blocks any outbound traffic until a secure connection is established. The best part: Cloak does that on the iPhone and iPad too.

Cloak is an app on iOS, and a menubar application on OS X, and costs as little as $2.99 a month for 5 GB of encrypted traffic; the Unlimited plan costs just $9.99 a month. (A 30-day trial is also available.)

If you already subscribe to another service, or your work uses a different VPN provider, you can configure the appropriate settings in the Network preference pane (under OS X) and the General > VPN settings (in iOS).

First Setup

If you haven't yet set up iCloud Keychain, you can do so on either your Mac or an iOS device.

1. On OS X, go to System Preferences, select the iCloud pane, and then scroll down in the list of services until you find Keychain. Click the checkbox next to it to enable the service **(4.14)**.

4.14 iCloud preferences on OS X

2. On your iOS device, go to Settings > iCloud, and tap Keychain. Then tap the switch to enable iCoud Keychain **(4.15)**.

4.15 Enabling iCloud Keychain on iOS

3. In both cases, you'll be prompted for your Apple ID password, and then asked to create an iCloud Security Code.

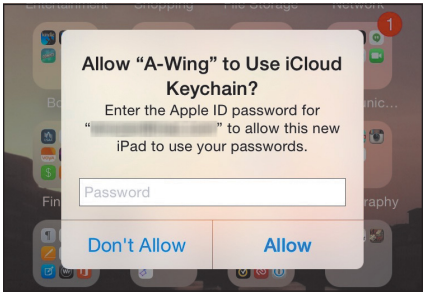
   By default, this code is a four-digit number, much like the passcode you might use for your iOS device. Using the Advanced options, you can also choose to get a random passcode or use a complex alphanumeric code. You can also opt to not create a security code at all: If you do so, Apple won't back your iCloud Keychain up to its server, which also means the company can't help you recover your keychain if it's damaged or otherwise becomes inaccessible. (Keep in mind that your keychain is stored on Apple's servers in encrypted form—the company never has access to your passwords, so it cannot retrieve them for you; the best it can do is help you restore your encrypted data.) However, iCloud Keychain information will continue to sync between devices that you've approved.

4. Enter an SMS-capable phone number at which you can receive verification codes via text. If you need to change this number later, you can do so on OS X via the Options button in the iCloud system preference pane, or on iOS via Settings > iCloud > Keychain > Advanced.

Subsequent Devices

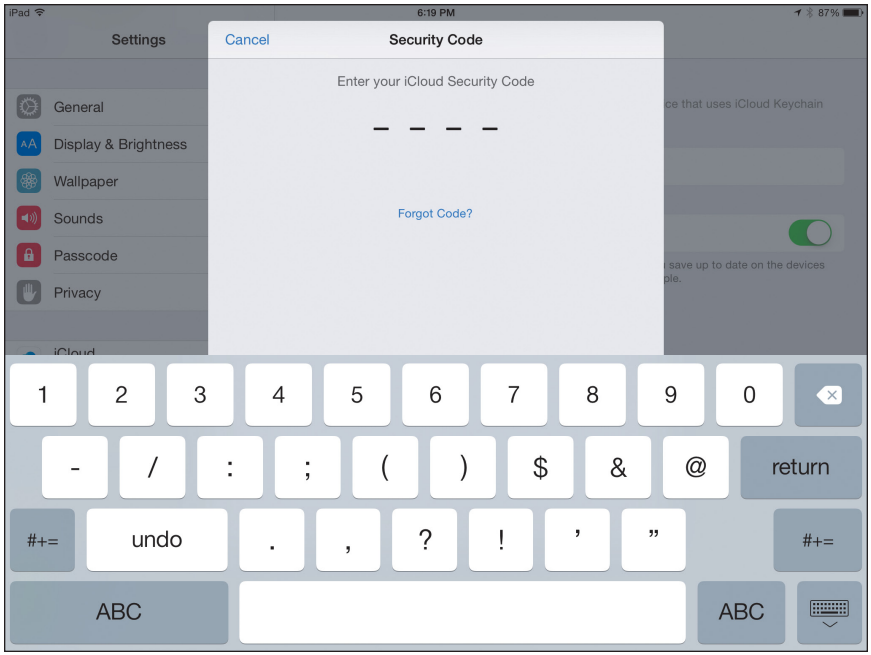
Once you've set up iCloud Keychain on one device, adding other devices is fairly straightforward. Follow the same steps to get to the iCloud settings of System Preferences (OS X) or Settings (iOS) and enable iCloud Keychain. You're then asked to approve the new device from an existing device that's already set up on iCloud Keychain **(4.16)**. A dialog appears on other devices already associated with iCloud Keychain, notifying you that a new device is seeking approval, along with a prompt to enter your iCloud password **(4.17)**.

4.16 Approving iCloud Keychain setup



4.17 Approval occurs on a separate device.

In those cases, you also have the option to approve a new device by entering the iCloud security code that you created, along with a verification code sent via SMS (4.18). While this might seem like a lot of steps to jump through, it's not unwarranted, given the amount of access it provides.



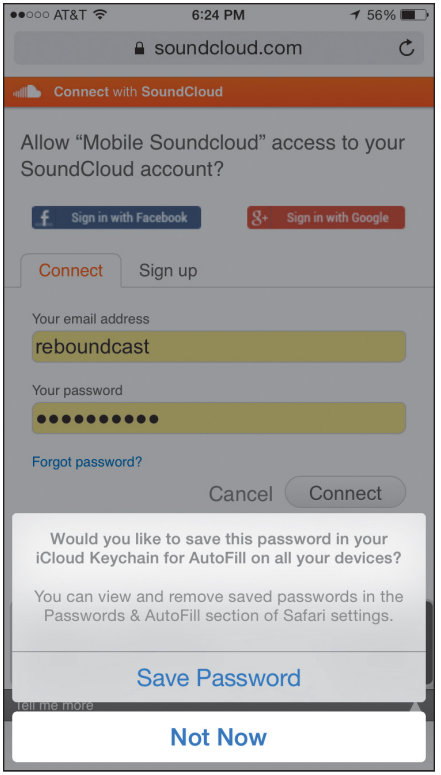
4.18 iCloud security code

Using iCloud Keychain

The primary place you'll likely encounter iCloud Keychain is Safari, though third-party apps can also connect with it. On OS X, you can also interact with it via the Keychain Access utility. Mostly, that interaction involves filling in usernames and passwords, but your iCloud Keychain can also store and recall credit card information.

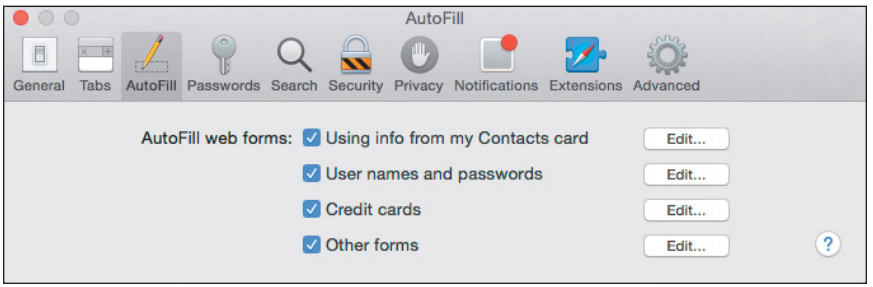
Usernames and passwords in iCloud Keychain

On either platform, when you encounter a username and password field in Safari and enter your credentials, a dialog asks if you want to save that password to your keychain (4.19). Doing so makes that information available on any other device using iCloud Keychain.



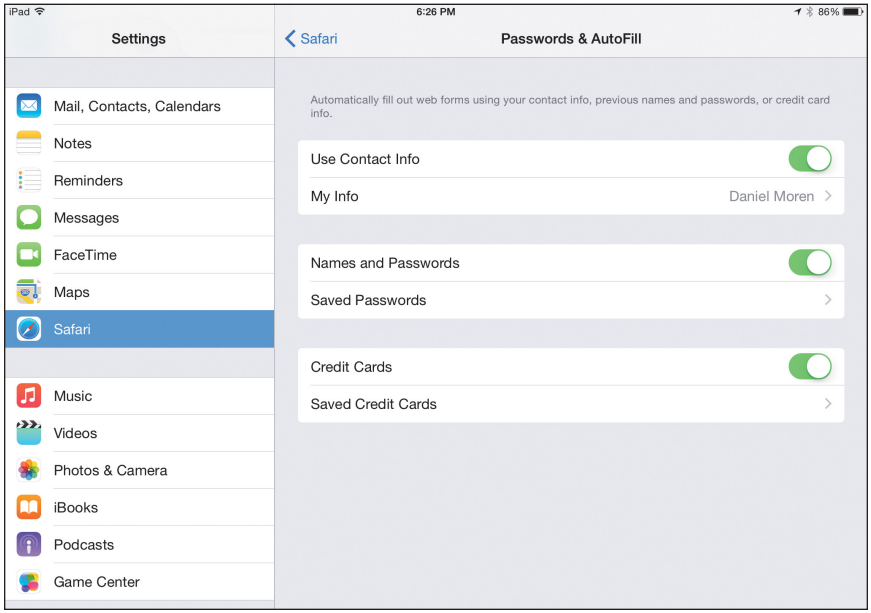
4.19 Saving a site password to iCloud Keychain

To fill in those passwords later, enable AutoFill. On OS X, go to the Safari menu and choose Preferences. Click AutoFill and click the box next to “user names and passwords.” **(4.20)** (You can also go to the Passwords section and select the checkbox next to AutoFill User Names and Passwords.)



4.20 Choosing AutoFill sources from iCloud Keychain

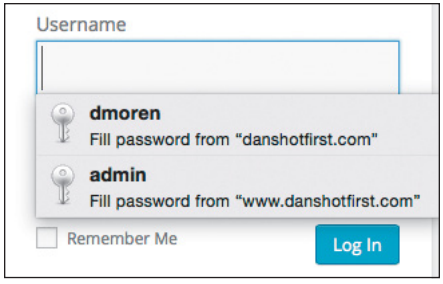
On iOS, go to Settings > Safari > Passwords & AutoFill and activate the slider next to Names and Passwords if it isn't already enabled (4.21).



4.21 Enabling AutoFill in Safari for iOS

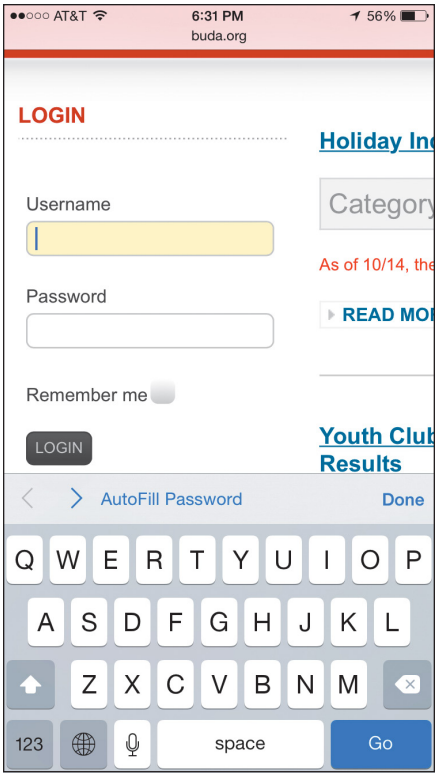
You can view or remove existing passwords from these locations, though it may require your passcode on iOS, and your username and password on OS X.

When Safari on iOS or OS X detects a site for which you've stored a username and password in your keychain, Safari automatically populates that information in the fields provided, which are highlighted in yellow. (If your keychain contains more than one username for that site, it provides a drop-down letting you pick which is the correct one (4.22).) In most cases, you can simply log in without any further intervention.



4.22 Multiple options for filling in username and password fields

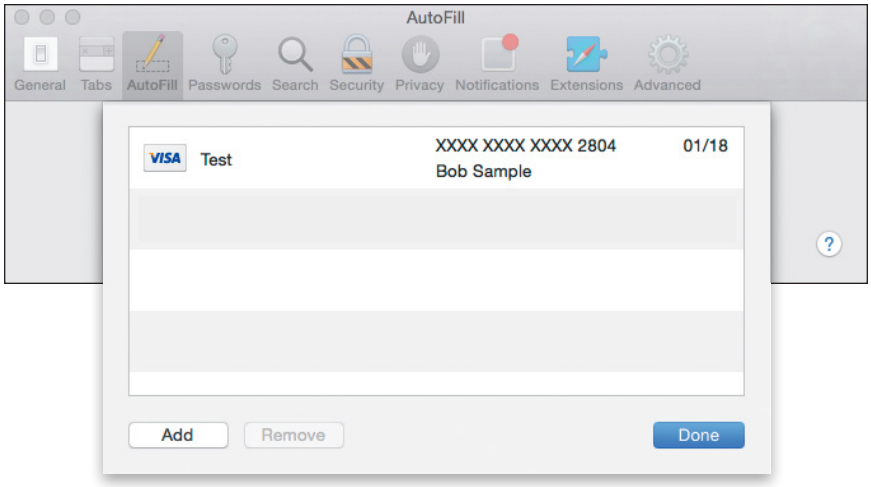
Sometimes, however, you may need to manually trigger AutoFill if Safari can't detect the field in question. On iOS, select a field and tap the AutoFill button that appears above the keyboard **(4.23)**. On OS X, you may need to click the field—sometimes Safari will then display an AutoFill dropdown.



4.23 AutoFill fields in OS X

Credit cards in iCloud Keychain

To enable AutoFill for credit cards on OS X, go to the AutoFill section of Safari's Preferences and click the box next to credit cards **(4.24, on the next page)**; on iOS, you'll find the option available in the Passwords & AutoFill section of Safari's settings. You can view or remove existing cards as well as add new cards here; to do any of those things on iOS, you'll have to enter your passcode—on OS X, you'll need to enter your username and password only to view an existing card's details.



4.24 Adding credit cards to AutoFill

For security reasons, Safari doesn't automatically populate credit card payments fields, even if you've stored a credit card in your keychain. You can tap the AutoFill button on iOS or click the field in OS X to enter that information, or choose from multiple cards if you have more than one.

▶ **NOTE** iCloud Keychain does not store the security code that appears on the back of your card—that makes it harder for someone to make unauthorized purchases if they compromise your keychain.

Removing a Device

Removing one of your devices from iCloud Keychain is as easy as revisiting System Preferences or Settings and deselecting or disabling iCloud Keychain. You're asked whether you'd like to keep the information currently stored on your device (**4.25**). If you retain that data, you can still use it, but it ceases updating between that device and your other devices.

4.25 Choosing what to do with stored data after turning off iCloud Keychain

If at any time you want to bring that device back into the iCloud Keychain fold, simply re-enable it following the steps mentioned earlier. To delete your iCloud Keychain data from Apple's servers, delete your iCloud Security Code and remove all your devices from iCloud Keychain.

1Password

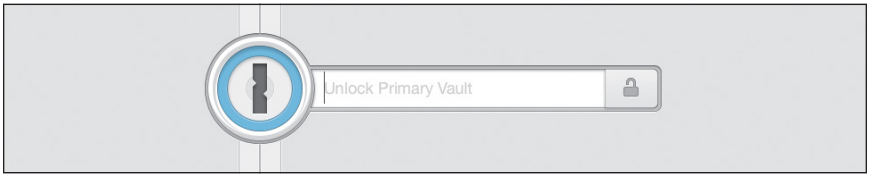
iCloud Keychain is a great solution for syncing your passwords: it's built into every Mac and iOS device, it works over iCloud, and it's free. But although it takes care of most basic password-storage needs, some folks will want a tool with more features or which allows use on non-Apple platforms.

Enter password managers. Several excellent third-party apps and services let you store passwords and other secure information for all of your accounts. Among the best is 1Password from Agile Bits, which is available for OS X from the developers' site or the Mac App Store, and on iOS from the App Store as a free download, though certain advanced features require an in-app purchase. You can use 1Password on just the Mac or just on iOS, but being able to sync data increases its usefulness exponentially.

We've used 1Password for years, before Apple implemented iCloud Keychain, so we have a lot of passwords and other information already stored. However, we don't ignore iCloud Keychain—it's better to have two secure options for important data than just one. Also, 1Password includes a few features iCloud Keychain doesn't.

In the Vault

1Password operates on the conceit of secure vaults (**4.26**). You create a vault, secured with a single master password, in which you store all your credentials for Web sites, account logins, credit cards, software licenses, and more. That way, the only thing you have to remember is the master password.



4.26 1Password on the Mac

When you open the app, you're prompted to create your first secure vault and specify a master password (4.27). Obviously, you'll want this master password to be especially memorable and secure, since it's the one password you'll want to remember. (And remember to make it distinct from your OS X account password, because reusing the same password is a no-no.)

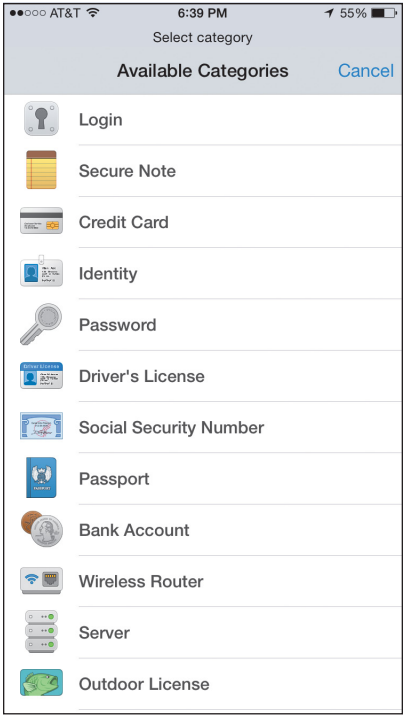
4.27 Creating a new 1Password vault

Once you've created your vault, start adding items. By default, 1Password offers a handful of common categories, including logins, secure notes, credit cards, and identities. Each of these comes preset with a number of fields tuned for that category of item. But if you tap or click the plus button to add a new item, you'll see a bunch of additional options, everything from your social security number to your outdoor license (4.28).

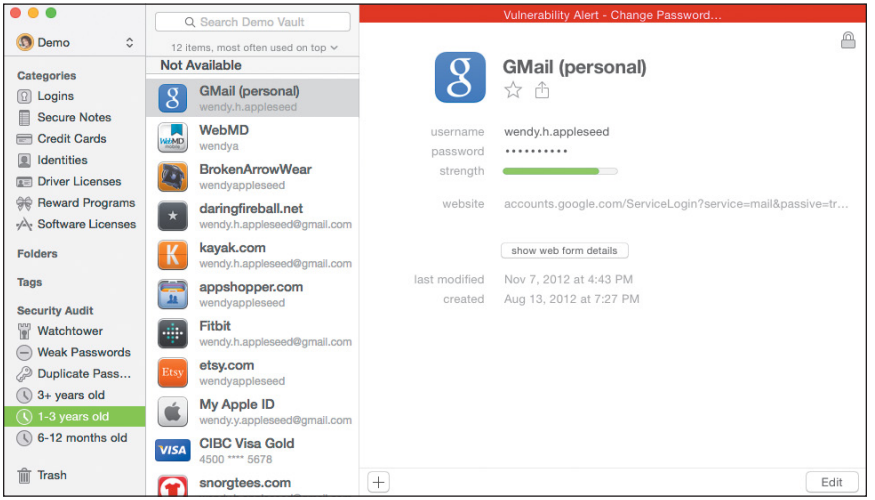
All of these items are fully searchable from within 1Password—except for the password field—just in case you remember, say, a URL, but not the name of the site. You can also organize your items into folders or tag them if you prefer, as well as mark the items that you find yourself frequently referring to as favorites.

On the Mac, 1Password even supports Smart Folders, letting you dynamically select items based on criteria that you specify—so, for example, if you want to see all the Web site passwords that haven't been updated in a year.

Though, honestly, you don't even have to go to that much trouble, because 1Password for OS X also has a Security Audit feature (4.29). This collects a variety of Smart Folders that not only let you quickly filter for passwords based on age, but also identify weak and duplicate passwords. And the Watchtower feature alerts you to sites on which your password may have been compromised, based on the latest information about security breaches.



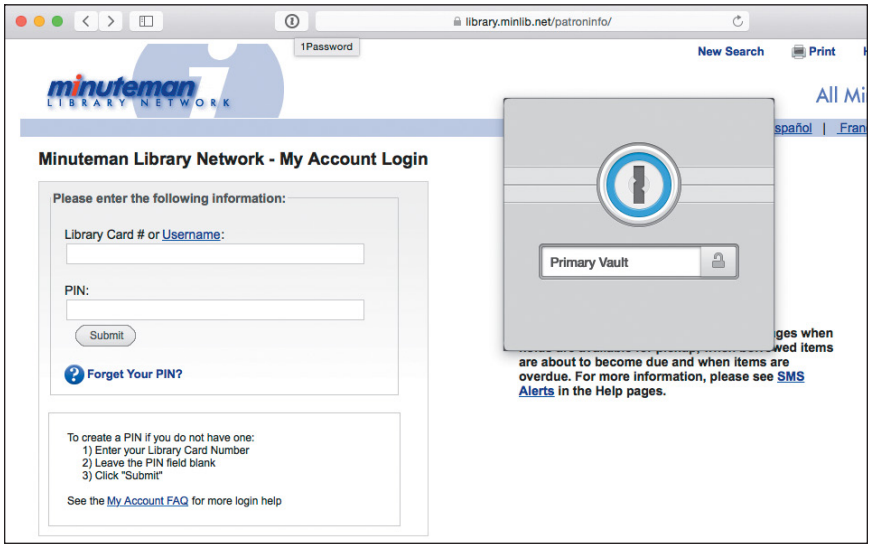
4.28 The types of data 1Password already has templates for



4.29 1Password Security Audit

Browser Integration

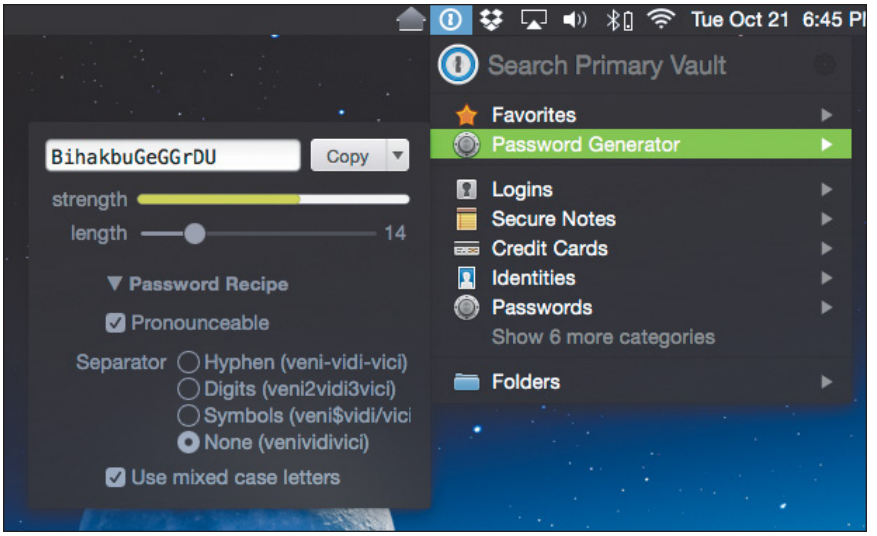
You'll probably spend most of your time using 1Password when you're in your Web browser of choice. The good news, then, is that it's extremely easy to use in conjunction with your browser: On OS X, the app includes extensions for both Chrome and Safari, each of which lets you summon the app with a user-defined keystroke. Once you've entered your master password, the 1Password extension automatically fills in the username and password for the site you're viewing **(4.30)**.



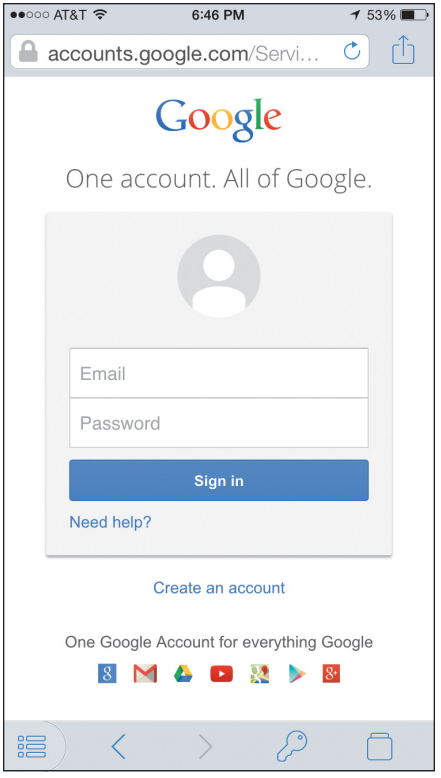
4.30 Accessing 1Password within Safari on OS X

When you create a new account on a Web site, 1Password on the Mac prompts you to add it to your records so you don't forget. And since you're entrusting all your passwords to your vault, 1Password includes a built-in password generator that helps you make complex, secure passwords. If you prefer, you can also access many of these features through 1Password mini, which lives in your Mac's menu bar **(4.31)**.

On the iOS side, you have multiple options. For one, the 1Password app includes its own secure browser, which provides integration with your database of passwords. Just tap the globe icon to access the browser **(4.32)**. When you reach a username and password field, tap the key icon in the toolbar to bring up your password information for that site, along with options for filling in credit cards or personal information.

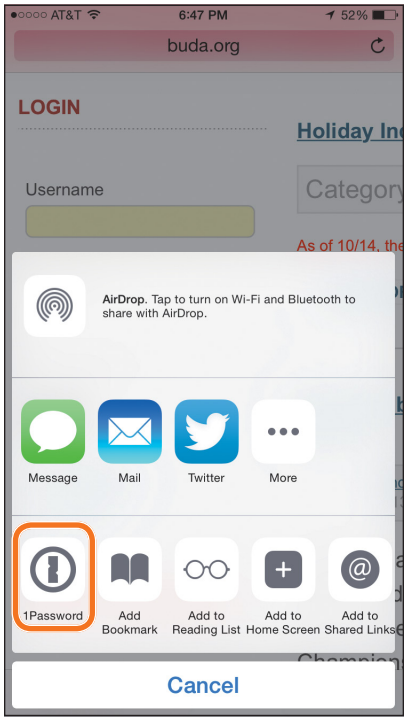


4.31 Generating a secure password in 1Password Mini



4.32 1Password's built-in secure browser on iOS

In iOS 8, however, the addition of extensions means that you can actually access 1Password from other apps, including Safari. Just bring up the Share menu and tap the 1Password option in the Action menu **(4.33)**. If a password is stored for that particular account, tap it to log yourself in, all without ever leaving the app.

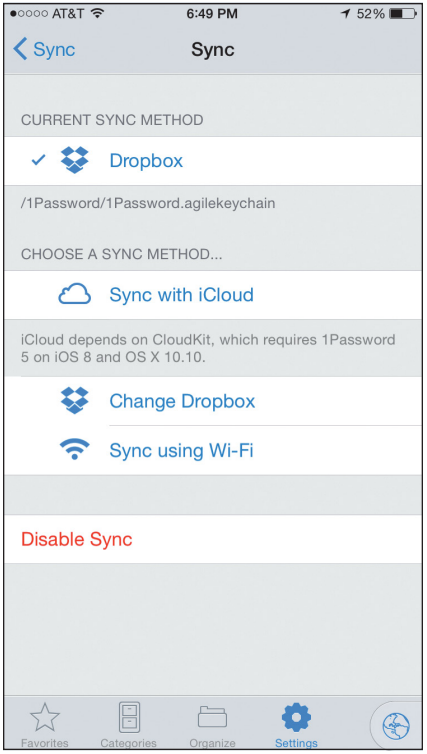


4.33 1Password logins in Safari for iOS

Syncing

The real benefit to a password manager, of course, is having all your passwords available at any time. 1Password allows you to sync information to all your devices, whether they're running iOS or OS X—or even, *gasp*, Windows and Android.

1Password provides four different methods of syncing your vault, depending on exactly how you use the app. Choose the one you want in 1Password's in-app Settings > Sync > Sync Service section if on iOS **(4.34)**, or the Sync section of 1Password's Preferences if you're on a Mac **(4.35)**.



4.34 Configuring Dropbox sync in iOS

4.35 Configuring Dropbox sync in Yosemite

If you're using only devices in Apple's ecosystem, iCloud syncing is easy to set up: Just select it as the service of choice on all your devices, and you're all set.

The second, and most broadly supported, option is Dropbox, which works with not only OS X and iOS, but also Windows, Windows Phone, and Android devices. You'll need to point the apps toward your vault in Dropbox, but once you've done that, it should sync just fine.

▶ **NOTE** If you don't have a Dropbox account, we highly recommend signing up for one at www.dropbox.com (you can get 2 GB of storage for free, or pay for larger capacities). Anything you put into your Dropbox folder is copied to the company's cloud service and to other computers on which you've set up the Dropbox software.

If you want to sync 1Password on your Mac with the iOS client, and you feel a bit wary about letting your information travel through a cloud storage service (even though the data is encrypted), you can opt to sync the two directly via Wi-Fi. Your devices, of course, have to be on the same Wi-Fi network, and you need to manually start the sync.

Finally, if you want to sync 1Password only via multiple computers, not via mobile devices, you can select any folder on your computer in which to store your vault; that folder can then be synced with any cloud storage service, not just Dropbox.

Multiple Vaults

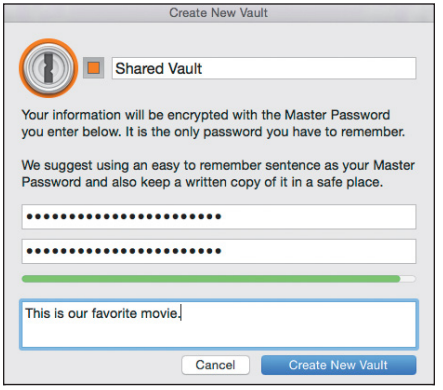
One handy feature of 1Password is support for multiple vaults. If you have more than one person sharing a computer (and they don't have their own user accounts), you can give each user their own vault, secured by their own master password; alternatively, if you want to separate secure information from, say, your work and your personal logins and passwords, you can create separate vaults and toggle between them.

Vaults can be synced independently, so, for example, if you find yourself doing tech support for certain members of your family—and you can convince them to use 1Password—you could set up a vault that you both have access to, making it easier to troubleshoot their problems when they arise. New vaults can be created only on OS X—but they can then be synced to 1Password on iOS. Here's how to set one up:

1. On the Mac, go to the 1Password menu and choose New Vault.
2. Specify a name for the vault, and pick an accent color to make it easy to distinguish.
3. Enter a master password to open the vault, which will be used by you and the other person **(4.36)**.
4. Click Create New Vault.
5. Go to 1Password > Preferences and click the Sync button.
6. Choose a sync method. iCloud can be used only for your Primary vault, so click Dropbox and choose a Dropbox folder to store the vault file. (The Dropbox folder needs to be one that you share with the other person; you can set up sharing after you finish creating the 1Password

vault.) If the other person's computer is on your home network and they don't need mobile syncing, choose the Folder option.

7. Click the Create New button to finish setting up the vault.



4.36 Creating a new shared vault

To add the shared vault to an iOS device (yours and the other person's), do this:

1. Go to Settings > Vaults and tap Add Vault.
2. Tap the Sync with Dropbox button. 1Password connects to your Dropbox account—you may have to grant it access.
3. Tap the name of your Dropbox account. 1Password scans the entire folder to locate any vaults.
4. In the list of saved vaults, tap the one you created in the previous steps.
5. Enter the vault's master password.

To switch between vaults in the 1Password app, go to Settings > Vaults and choose the one you want. On the Mac, choose a vault from the drop-down above the category list.

▶ **TIP** Create a new entry in your Primary vault that includes the password to the vault you created, to make sure you have a record of that password.

▶ **TIP** On the Mac, you can copy or move 1Password entries between vaults, making it easier to share items you have in common (such as online access to a joint bank account). Select a record and choose Item > Share, then choose the vault from the submenu that appears, and select Copy or Move.

Find a Lost Device

Losing a digital device can be a traumatic experience. While the devices themselves are expensive to replace, the information on them is all too often irreplaceable. Fortunately, the same technology that makes these devices so useful can also be turned toward bringing an errant device home—even if it had only fallen between the couch cushions.

Enabling Find My iPhone/iPad/iPod/Mac

The good news is that most of the devices that you might misplace come with ways of locating themselves. iPhones contain GPS chips, while iPads, iPod touches, and Macs can all locate themselves based on nearby Wi-Fi networks.

To take advantage of this feature, you'll need to activate Find My iPhone (or iPad, iPod, or Mac, depending on which device you're using), the service that reports in on the devices' locations **(4.37)**. On iOS, this is in Settings > iCloud; on OS X, the service is called Find My Mac and is located in the iCloud preference pane of System Preferences **(4.38)**.

When you activate the service, you're asked to allow the device's location to be reported via the service; tap or click Allow. (If you enabled Find My [Device] when you set up the device, it's already running.)

4.37 Activating Find My Mac in Yosemite

4.38 Activating Find My iPhone in iOS

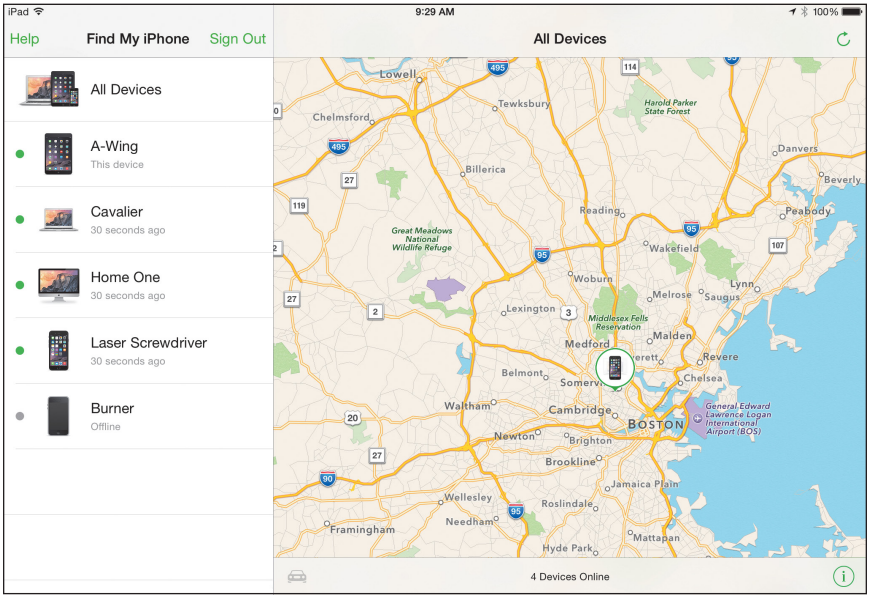
iOS devices also have one additional option once the service is activated: Send Last Location. When your device's battery runs low, it'll send its last known location to Apple's servers—that way you should be able to locate your device even if it's out of juice.

Finding a Device

The most important thing to do when you lose a device is stay calm. As soon as possible, try to access the Find My iPhone service and locate your device.

If you have an iOS device available—either yours or somebody else's—use Apple's free Find My iPhone app to locate your errant gadget. (Don't be fooled by the name: It'll help you locate iPads, iPods, and Macs too, as long as you've followed the above steps to enable the service on those devices.)

1. Launch the Find My iPhone app, and enter the iCloud account and password with which the missing device is associated. (On somebody else's device, you may need to tap the Sign Out button and sign in with your iCloud account.) You'll see a map and, if you have more than one machine registered with the service, a list of all the available Macs and iOS devices, along with when their location was last reported **(4.39)**. By default, their locations are shown on the map.

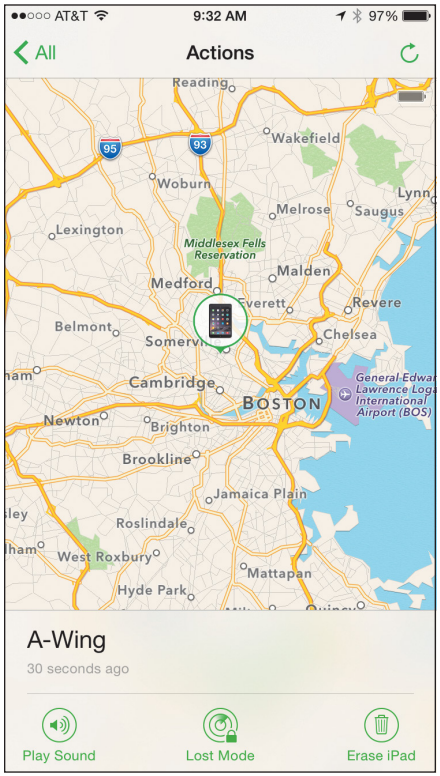


4.39 It's right there. I'm pointing right at it.

2. Select any single device to see just that device's location and status.

Once you select a device, you have a number of options.

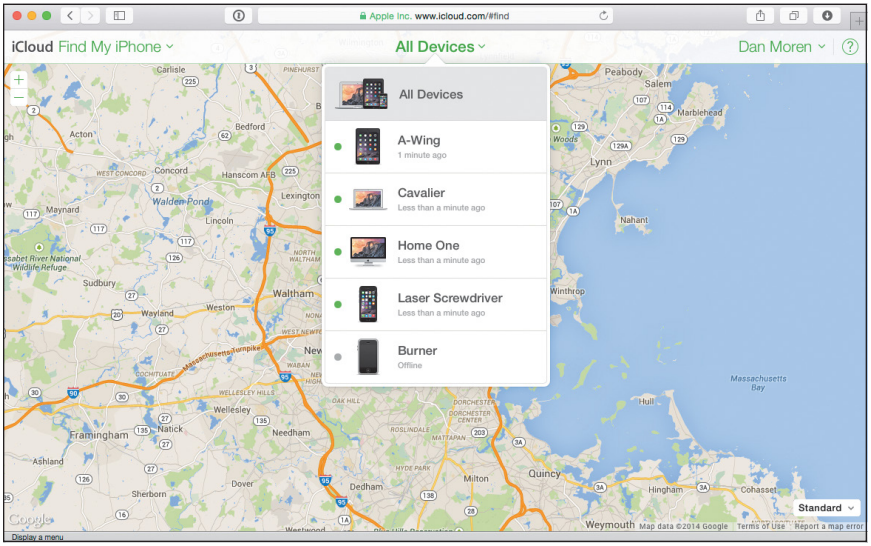
- To quickly plot driving directions via the Maps app, tap the car icon at the bottom left of the map.
- Tap Actions to bring up a toolbar of other options, including Play Sound (which works even if the device in question is muted), the ability to erase the device, and either activating Lost Mode (for an iOS device) or locking the machine (for a Mac) (**4.40**). Play Sound is usually sufficient for us to find where the device has run off to.



4.40 Options for finding a lost device

If you don't have an iOS device handy but do have a computer, you can perform all of these functions from Apple's iCloud Web site. Just go to www.icloud.com, enter your username and password, and select the Find

My iPhone icon. You'll find the same options as you would have on an iOS device **(4.41)**.



4.41 Find My iPhone at iCloud.com

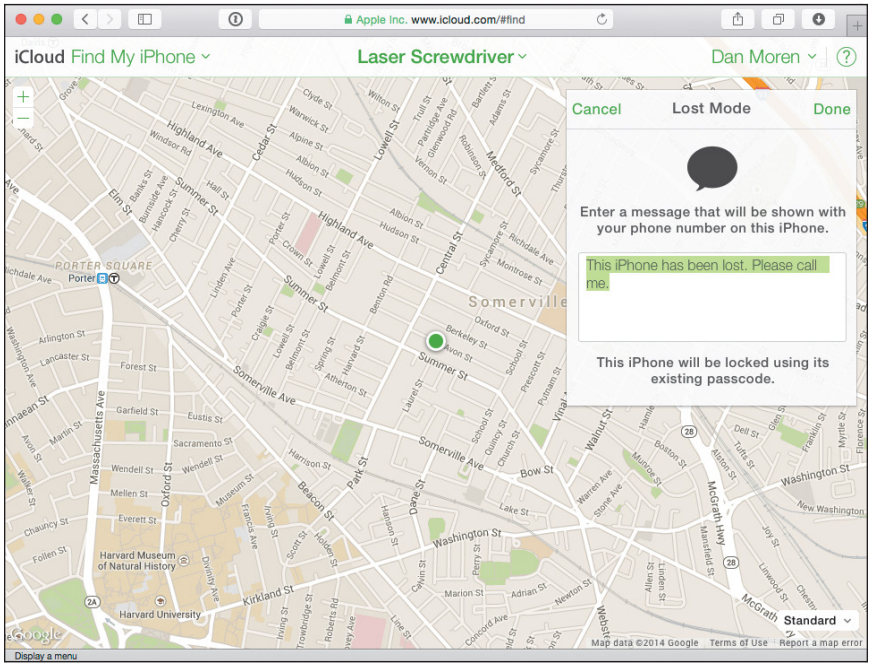
Lost Mode

If you've truly misplaced your iOS device or suspect that it may have been stolen, activating Lost Mode can help you track it, as well as lock it so that it's inaccessible. Use the Find My iPhone app or iCloud Web site to turn Lost Mode on.

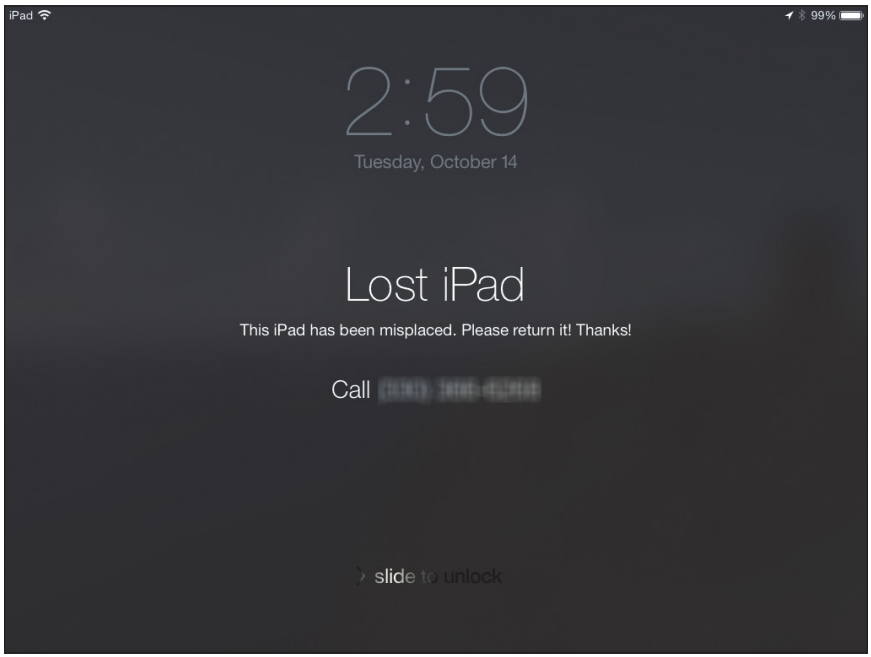
Once you've activated it, you can optionally enter a phone number, which is displayed on the iPad. (If it's your iPhone that you've misplaced, remember that you'll want to use another phone number, such a friend's or family member's.) You'll also be asked to enter a message that's shown along with the number **(4.42, on the next page)**.

Once you tap Done, your iOS device is placed into Lost Mode: The device is immediately locked if it's currently active, and the lock screen permanently displays the message you entered, along with the phone number you provided **(4.43, on the next page)**. If the lost device is an iPhone, a Call button on the lock screen lets someone quickly contact you at the number you specified.

4.42 Lost Mode



4.43 Not all who wander are lost—except this iPad, which is clearly lost. Please help it find its way home.



While in Lost Mode, your device's movements are also tracked and reported in the Find My iPhone app and Web site. Whenever its location is updated, an email is sent to your address with the last known location.

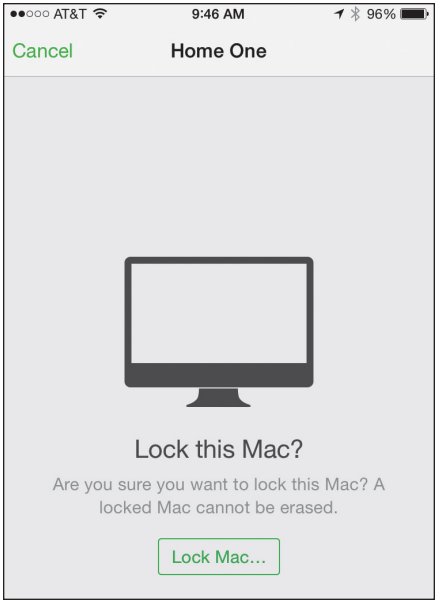
You can update the phone number or message by selecting the device in Find My iPhone and tapping Lost Mode again—you can also use that screen to turn off Lost Mode once your device has been located. Unlocking an iOS device with your passcode or via Touch ID automatically terminates Lost Mode.

Tip If you suspect your device was stolen, and you locate it on the map, don't attempt to retrieve it yourself. Call the police. Security also applies to keeping yourself out of harm's way.

Lock Your Mac

Much like Lost Mode, locking your Mac provides a way to prevent anybody from using your computer if it's misplaced. You can activate it once you've selected a Mac in Find My iPhone on an iOS device or on the Web **(4.44)**.

▶ **NOTE** A locked Mac, as Find My iPhone will warn you, cannot be erased. Therefore, think carefully before locking it if sensitive data is on your disk—especially if it's not encrypted with FileVault (see earlier).



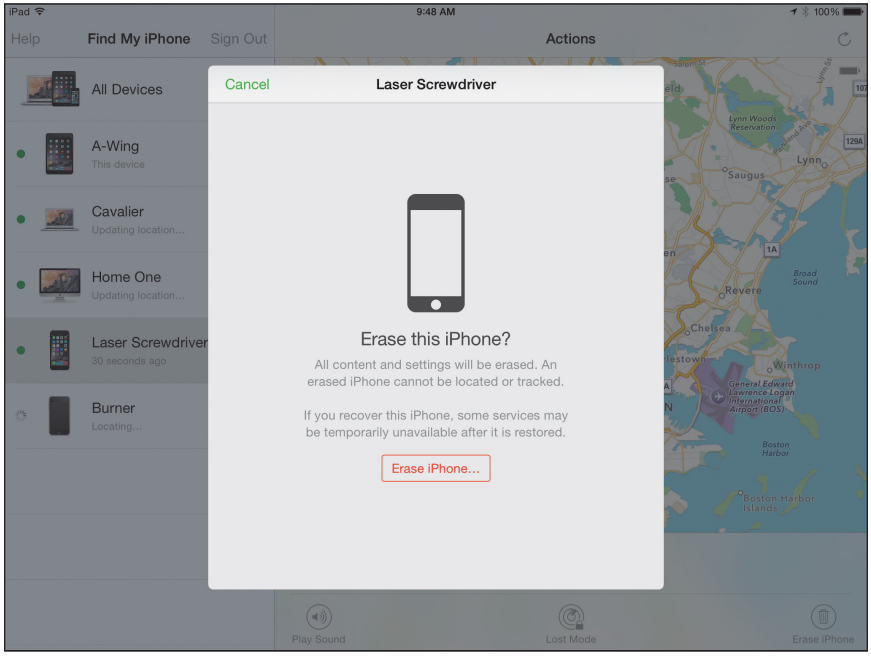
4.44 Locking a Mac remotely

When you lock your Mac remotely, you're asked to enter and confirm a four-digit code, as well as provide a message that is shown on the Mac. Once you've done that and locked the Mac, the lost computer is restarted and you're sent an email notifying you that the computer has been locked to a passcode—the passcode itself, however, is not provided, so make sure it's one you remember or stored in a secure location.

Once the Mac restarts, you have to enter the code you created before you can log in; entering the pin will unlock the Mac. Keep in mind, however, that if your disk is not encrypted with FileVault, someone could boot the machine from an external drive to get access to that information.

Erase Device

If there's really no hope of recovering a lost device, you may want to consider erasing it, which ensures that any information stored is inaccessible. Be aware that erasing a device is irreversible, and once you do so, you won't be able to play a sound, lock it, put it in Lost Mode, or locate it via Find My iPhone **(4.45)**.



4.45 Erasing a lost iPhone

In theory, erasing your device shouldn't be too much of a concern, as long as you have a current backup, either via iCloud Backup or iTunes for iOS devices, or Time Machine or one of the many other third-party solutions on the Mac. You do have a backup, don't you? (See Chapter 6.)

Selecting a device and choosing Erase Device prompts you for your Apple ID password and, as with Lost Mode or locking your Mac, also asks for a phone number and a message that will be displayed on the device after it's erased. In the case of your Mac, you'll also be asked to create a passcode that will be needed to unlock it.

How soon the erase takes effect depends on whether the device is currently online; if it is, the remote wipe starts working immediately. Otherwise, erasure begins the next time the device connects to the Internet. The process of erasing can also take some time: a Mac, for example, can take up to a day.

If you erase a device with cellular service, keep in mind that you will likely want to notify your service provider to suspend the device, just in case someone attempts to use it.

Third-Party Tools

Find My iPhone can only do so much. If you're looking for a tool to help track down the person who stole your device, you may wish to consider a third-party option.

Orbicule's Undercover (www.orbicule.com) not only helps you locate a stolen Mac, but it can also use your computer's built-in camera to take and send pictures, perhaps helping you locate or identify the perpetrator, as well as logging their keystrokes and taking periodic screenshots.

Hidden (www.hiddenapp.com) is another OS X app that, similar to Undercover, can track your stolen Mac, take photos with the camera, snap screenshots, log keystrokes, and let you remotely wipe your computer. It also allows you send messages that your computer will speak aloud, create a reverse secure connection, and more.

Prey Anti Theft (preyproject.com), which runs on both iOS or OS X, is a free option for up to three of your devices. It helps you locate your missing device, as well as providing you with information about the device's use.

This page intentionally left blank

INDEX

Numbers

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

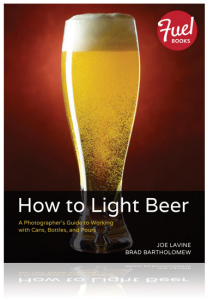
Y

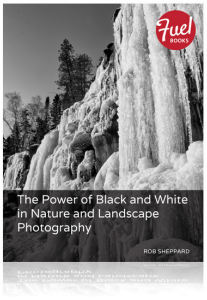
INTRODUCING

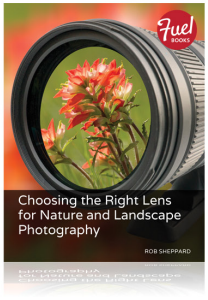
Fuel BOOKS

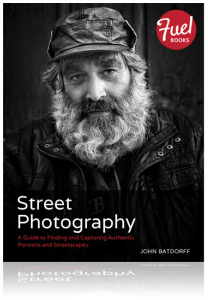
Powerful Ideas. Inspired eBooks.

Need a little boost? Then fill up on Fuel! Packed with practical tools and tips that will help you quickly advance your creative skills, these short eBooks get right to the heart of what you need to learn. Every FuelBook comes in three formats—MOBI, ePUB, and an elegantly laid out PDF—so you can choose the reading experience that works best for you on whatever device you choose. Written by top authors and trainers, FuelBooks offer friendly, straightforward instruction and innovative ideas to power your creativity.









For a free sample and more information, visit: fuelbooks.com